

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-302393

(43) 公開日 平成10年(1998)11月13日

(51) Int.Cl.⁹
 G 1 1 B 20/10
 G 0 6 F 12/14
 G 0 9 C 1/00

識別記号
 3 2 0
 6 6 0

F I
 G 1 1 B 20/10
 G 0 6 F 12/14
 G 0 9 C 1/00

H
 3 2 0 E
 3 2 0 B
 6 6 0 D

審査請求 未請求 請求項の数14 O L (全 11 頁)

(21) 出願番号 特願平9-107541

(22) 出願日 平成9年(1997)4月24日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 加藤 岳久

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 遠藤 直樹

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 下田 乾二

神奈川県横浜市磯子区新杉田町8番地 株式会社東芝横浜事業所内

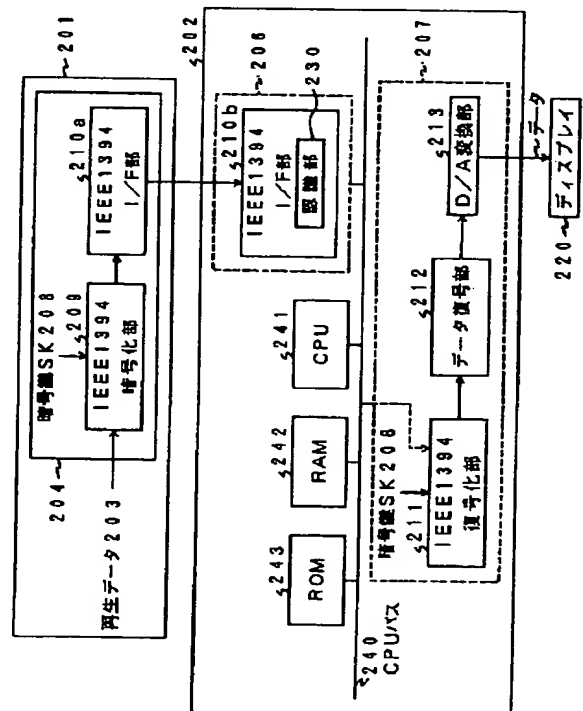
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 不正コピーを防止する方法、及びその半導体装置並びにデジタル記録再生システム

(57) 【要約】

【課題】 AV機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっては、CPUバス上を流れるデータのコピーによる不正なコピーを防止する。

【解決手段】 送信側と受信側とで暗号データを伝送する場合に、その送受信インターフェースとして、専用デジタル機器と、コンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル機器での不正コピーを防止する方法において、受信側に用いられる機器が専用デジタル機器であるか、汎用デジタル機器であるかに対応して構成される統一規格の受信側 I/F 手段が、何れのデジタル機器に対応するかが認識され、受信側 I/F 手段がその対応するデジタル機器に設けられているときのみ、送信側と受信側とで正常なデータ伝送を行う不正コピーを防止する方法。



【特許請求の範囲】

【請求項 1】 暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信インターフェースとして、オーディオビジュアル機器等の専用デジタル機器と、ソフトウェアでコントロール可能な CPU バスをもつコンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル記録再生システムにおいて、

前記受信側に用いられる機器が前記専用デジタル機器であるか、前記汎用デジタル機器であるかに対応して構成され、かつ前記送受信インターフェースに対応して構成される受信側 I/F 手段と、

前記受信側 I/F 手段と一体にして設けられ、かつ前記受信側 I/F 手段が何れのデジタル機器に対応するかを認識可能とする認識手段とを備え、前記受信側 I/F 手段がその対応するデジタル機器に設けられているときのみ、前記送信側と前記受信側とで正常なデータ伝送を行うことを可能としたことを特徴とするデジタル記録再生システム。

【請求項 2】 前記受信側 I/F 手段が前記汎用デジタル機器に対応する場合において、暗号が解読されたデータを再生出力するデータ再生出力手段と、

前記受信側 I/F 手段から前記 CPU バスを介してデータ転送された転送先に設けられ、かつ前記 CPU バスを介することなく前記データ再生出力手段にデータ出力するデータ処理手段と、

前記データ処理手段に設けられ、かつ前記暗号化されたデータを暗号解読する復号手段とを備えたことを特徴とする請求項 1 記載のデジタル記録再生システム。

【請求項 3】 前記送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、前記受信側には、圧縮されたデータを解凍する手段が設けられたことを特徴とする請求項 1 又は 2 記載のデジタル記録再生システム。

【請求項 4】 前記受信側 I/F 手段を構成する半導体装置は、前記専用デジタル機器に対応するものと、前記汎用デジタル機器に対応するもので、形状が異なり相互の交換が不可であることを特徴とする請求項 1 乃至 3 のうち何れか 1 項記載のデジタル記録再生システム。

【請求項 5】 前記受信側 I/F 手段を構成する半導体装置は、前記専用デジタル機器に対応するものと、前記汎用デジタル機器に対応するもので、その内部処理用のコードが異なり相互の交換が不可であることを特徴とする請求項 1 乃至 4 のうち何れか 1 項記載のデジタル記録再生システム。

【請求項 6】 暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信

側との間の送受信インターフェースとして、オーディオビジュアル機器等の専用デジタル機器と、ソフトウェアでコントロール可能な CPU バスをもつコンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル機器での不正コピーを防止する方法において、

前記受信側に用いられる機器が前記専用デジタル機器であるか、前記汎用デジタル機器であるかに対応して構成され、かつ前記送受信インターフェースに対応して構成される受信側 I/F 手段が、何れのデジタル機器に対応するかが認識され、

前記受信側 I/F 手段がその対応するデジタル機器に設けられているときのみ、前記送信側と前記受信側とで正常なデータ伝送を行うことを特徴とする不正コピーを防止する方法。

【請求項 7】 前記受信側 I/F 手段が前記汎用デジタル機器に対応する場合において、

前記受信側 I/F 手段にて受信された前記暗号化されたデータが前記 CPU バスを介して転送され、

この転送先にて前記暗号化されたデータを暗号解読し、前記 CPU バスをこれ以上介することなく解読されたデータを出力することを特徴とする請求項 6 記載の不正コピーを防止する方法。

【請求項 8】 前記送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、前記受信側にて圧縮されたデータが解凍されることを特徴とする請求項 6 又は 7 記載の不正コピーを防止する方法。

【請求項 9】 暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信インターフェースとして、オーディオビジュアル機器等の専用デジタル機器と、ソフトウェアでコントロール可能な CPU バスをもつコンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル機器に使用される半導体装置において、

前記受信側に用いられる機器が前記専用デジタル機器であるか、前記汎用デジタル機器であるかに対応して構成され、かつ前記送受信インターフェースに対応して構成される I/F 手段と、

前記 I/F 手段が何れのデジタル機器に対応するかを認識可能とする認識手段とを備えたことを特徴とする半導体装置。

【請求項 10】 前記 I/F 手段が前記専用デジタル機器に対応する受信側 I/F 手段である場合において、前記暗号化されたデータを暗号解読する復号手段を備えたことを特徴とする請求項 9 記載の半導体装置。

【請求項 11】 前記専用デジタル機器に対応するものと、前記汎用デジタル機器に対応するもので、形状が異なり相互の交換が不可であることを特徴とする請求項 9 又は 10 記載の半導体装置。

【請求項 12】 前記専用デジタル機器に対応するものと、前記汎用デジタル機器に対応するものとで、その内部処理用のコードが異なり相互の交換が不可であることを特徴とする請求項 9 乃至 11 のうち何れか 1 項記載の半導体装置。

【請求項 13】 外部より入力したデータ若しくは内部の記録媒体から読み出したデータを暗号化処理する暗号化手段と、この暗号化手段により暗号化された前記データを外部伝送路に出力する送信手段とを有する送信側機器と、

前記外部伝送路を介して前記暗号化されたデータを受信する受信手段と、この受信手段により受信した前記暗号化されたデータの復元化処理を行う復号化手段とを有する受信側機器とからなる情報提供システムにおいて、前記送信手段は前記受信手段と交信することにより、受信側機器を認識する認識手段を備え、前記送信手段は前記認識手段が受信側機器が送信可能な機器であると認識した場合にのみ前記データの送信を行うことを特徴とする情報提供システム。

【請求項 14】 前記受信側機器は、オーディオビジュアル機器等の専用デジタル機器がソフトウェアによりコントロール可能な CPU バスを有するコンピュータ等の汎用デジタル機器の何れか一方であり、前記認識手段は受信側機器が専用デジタル機器か汎用デジタル機器であるかを認識することを特徴とする請求項 13 記載の情報提供システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は不正コピーを防止する方法、及びその半導体装置並びにシステム、更に詳しくはデジタル化された文書、音声、画像、プログラム等の圧縮されたデータの不正コピーを防止する部分に特徴のある不正コピーを防止する方法、及びその半導体装置並びにデジタル記録再生システムに関するものである。

【0002】

【従来の技術】最近、マルチメディアの発展に伴って機器のネットワーク化が進み、パーソナルコンピュータ等の汎用計算機間のみならず、オーディオ機器やビデオ機器等のオーディオビジュアル機器（AV 機器）とのデータの送受信、ケーブルテレビや衛星放送のデジタル化等、データのデジタル化、ネットワーク化が一般的になりつつある。

【0003】そこで、コンピュータと AV 機器等のデジタル機器との間でデータの送受信を行うためのデジタルインターフェース方式の統一規格が検討されている。その中の一つに IEEE 1394 がある。この IEEE 1394 については、例えば新エレクトロニクス文庫（2）『次世代シリアルインターフェース IEEE1394 がわかる本』エレクトロニクス 1997 年 1 月号付録、オーム

社、に詳述されている。

【0004】一方、近年デジタル記録再生機器の開発、製品化が進み、画質や音質の劣化なくデータをコピーすることが可能となっている。しかし高画質な複製は、海賊版と呼ばれる不正なコピーを増加させ、著作権が侵害されるという問題がある。このような不正なコピーは確実に防止されなければならない。というのも、インターネットやデジタル VTR や DVD-RAM の出現により、デジタル化された著作物は簡単にコピーされ、不特定多数への配布が可能となり、これによりデジタル画像の著作権者に危機感を与えているからである。

【0005】このため、従来は、データを暗号化して通信または記録保存、読み出しをする暗号化通信または暗号化システムを用いることでこのような不正コピーを防止していた。

【0006】

【発明が解決しようとする課題】しかしながら、デジタル化された文書、音声、画像、プログラムなどの圧縮されたマルチメディア・データをネットワークやケーブルを介して通信を行うデジタル記録再生システム、また上記デジタルデータを記録保存、読み出しするデジタル記録再生システムにおいては、専用機器である AV 機器のみならず汎用性の高い計算機もが用いられることで次のような問題が発生する。

【0007】すなわち、パーソナルコンピュータ（以下、パソコンともいう）のような汎用計算機を通してマルチメディア・データを再生する場合には、CPU バスを介してデータを処理するため、たとえ上記暗号化技術が用いられていても、暗号が解除された表示出力前の CPU バスを流れるデータコピーすることが可能となる。

【0008】したがって、ソフトウェア手段でパソコンを制御すれば、上記マルチメディア・データを容易にコピーすることができ、不正なコピーが可能となる。このように、IEEE 1394 等のインターフェースを用いて著作物を流通させた場合、パソコン等の計算機が不正コピーを助長するものになってしまう。

【0009】また、コンピュータと AV 機器等とのデジタルインターフェース方式の統一規格である IEEE 1394 は、その汎用性から広く普及するものと予想されるが、その時にはコンピュータと AV 機器等との組み合わせの場合のみでなく、コンピュータのみの場合や AV 機器等のみの場合であっても IEEE 1394 が使用されるものと考えられる。

【0010】かかる状況にあつては、上記したようにパソコンを使用した場合の不正コピー防止のみならず、コンピュータと AV 機器との全体を考慮した不正コピー防止対策を講じなければならない。さもなければ IEEE 1394 における、コンピュータと AV 機器等との統一規格としての意義が失われるからである。

【0011】本発明は、このような実情を考慮してなされたもので、A/V機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっては、CPUバス上を流れるデータのコピーによる不正なコピーを防止することが可能な不正コピーを防止する方法、及びその半導体装置並びにデジタル記録再生システムを提供することを目的とする。

【0012】

【課題を解決するための手段】上記課題を解決するために、請求項1に対応する発明は、暗号化されたデータを送信する送信側と前記暗号化されたデータを受信し復号して出力する受信側との間の送受信インターフェースとして、オーディオビジュアル機器等の専用デジタル機器と、ソフトウェアでコントロール可能なCPUバスをもつコンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル記録再生システムにおいて、受信側に用いられる機器が専用デジタル機器であるか、汎用デジタル機器であるかに対応して構成され、かつ送受信インターフェースに対応して構成される受信側I/F手段と、受信側I/F手段と一体にして設けられ、かつ受信側I/F手段が何れのデジタル機器に対応するかを認識可能とする認識手段とを備え、受信側I/F手段がその対応するデジタル機器に設けられているときのみ、送信側と受信側とで正常なデータ伝送を行うことを可能としたデジタル記録再生システムである。

【0013】本発明は、このような手段を設けたので、受信側に用いられる機器が専用デジタル機器であるか、汎用デジタル機器であるかが確実に区別されることとなり、正規な機器が用いられない場合にはデータ伝送できない。

【0014】したがって、オーディオビジュアル機器等と計算機等との何れもが使用され得る状況にあっては、これらの機器に対して適切な暗号化がなされていれば、少なくともオーディオビジュアル機器等における不正コピーを防止できるとともに、オーディオビジュアル機器等と計算機等との混在使用を防止でき、ひいてはCPUバス上を流れるデータのコピーによる不正なコピーを防止する手段を講じることが可能となる。

【0015】また、請求項2に対応する発明は、請求項1に対応する発明において、受信側I/F手段が汎用デジタル機器に対応する場合において、暗号が解読されたデータを再生出力するデータ再生出力手段と、受信側I/F手段からCPUバスを介してデータ転送された転送先に設けられ、かつCPUバスを介することなくデータ再生出力手段にデータ出力するデータ処理手段と、データ処理手段に設けられ、かつ前記暗号化されたデータを暗号解読する復号手段とを備えたデジタル記録再生システムである。

【0016】本発明は、このような手段を設けたので、請求項1に対応する発明と同様な作用効果が得られる他、オーディオビジュアル機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっては、CPUバス上を流れるデータのコピーによる不正なコピーを防止することができる。

【0017】さらに、請求項3に対応する発明は、請求項1又は2に対応する発明において、送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、受信側には、圧縮されたデータを解凍する手段が設けられたデジタル記録再生システムである。

【0018】本発明は、このような手段を設けたので、データ圧縮を行う場合にあっては、請求項1又は2に対応する発明と同様な作用効果が得られる。さらにまた、請求項4に対応する発明は、請求項1～3に対応する発明において、受信側I/F手段を構成する半導体装置は、専用デジタル機器に対応するものと、汎用デジタル機器に対応するものとで、形状が異なり相互の交換が不可であるデジタル記録再生システムである。

【0019】本発明は、このような手段を設けたので、請求項1～3に対応する発明と同様な作用効果が得られる他、チップ等の半導体装置を交換することによる不正コピーを防止することができる。

【0020】一方、請求項5に対応する発明は、請求項1～4に対応する発明において、受信側I/F手段を構成する半導体装置は、専用デジタル機器に対応するものと、汎用デジタル機器に対応するものとで、その内部処理用のコードが異なり相互の交換が不可であるデジタル記録再生システムである。

【0021】本発明は、このような手段を設けたので、請求項1～4に対応する発明と同様な作用効果が得られる他、より一層確実に半導体装置を交換することによる不正コピーを防止することができる。

【0022】次に、請求項6に対応する発明は、暗号化されたデータを送信する送信側と暗号化されたデータを受信し復号して出力する受信側との間の送受信インターフェースとして、オーディオビジュアル機器等の専用デジタル機器と、ソフトウェアでコントロール可能なCPUバスをもつコンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル機器での不正コピーを防止する方法において、受信側に用いられる機器が専用デジタル機器であるか、汎用デジタル機器であるかに対応して構成され、かつ送受信インターフェースに対応して構成される受信側I/F手段が、何れのデジタル機器に対応するかが認識され、受信側I/F手段がその対応するデジタル機器に設けられているときのみ、送信側と受信側とで正常なデータ伝送を行う不正コピーを防止する方法である。

【0023】本発明は、このような手段を設けたので、請求項1に対応する発明と同様な作用効果が得られる。また、請求項7に対応する発明は、請求項6に対応する発明において、受信側I/F手段が汎用デジタル機器に対応する場合において、受信側I/F手段にて受信された暗号化されたデータがCPUバスを介して転送され、この転送先にて暗号化されたデータを暗号解読し、CPUバスをこれ以上介することなく解読されたデータを出力する不正コピーを防止する方法である。

【0024】本発明は、このような手段を設けたので、請求項2に対応する発明と同様な作用効果が得られる。さらに、請求項8に対応する発明は、請求項6又は7に対応する発明において、送信側から出力する暗号化されたデータにはデータ圧縮がかけられており、受信側にて圧縮されたデータが解凍される不正コピーを防止する方法である。

【0025】本発明は、このような手段を設けたので、請求項3に対応する発明と同様な作用効果が得られる。さらにまた、請求項9に対応する発明は、暗号化されたデータを送信する送信側と暗号化されたデータを受信し復号して出力する受信側との間の送受信インターフェースとして、オーディオヴィジュアル機器等の専用デジタル機器と、ソフトウェアでコントロール可能なCPUバスをもつコンピュータ等の汎用デジタル機器との両者を扱い可能とする統一規格に従うインターフェースを用いたデジタル機器に使用される半導体装置において、受信側に用いられる機器が専用デジタル機器であるか、汎用デジタル機器であるかに対応して構成され、かつ送受信インターフェースに対応して構成されるI/F手段と、I/F手段が何れのデジタル機器に対応するかを認識可能とする認識手段とを備えた半導体装置である。

【0026】本発明は、このような手段を設けたので、請求項1に対応する発明と同様な作用効果が得られる。一方、請求項10に対応する発明は、請求項9に対応する発明において、I/F手段が専用デジタル機器に対応する受信側I/F手段である場合において、暗号化されたデータを暗号解読する復号手段を備えた半導体装置である。

【0027】本発明は、このような手段を設けたので、請求項9に対応する発明と同様な作用効果が得られる。次に、請求項11に対応する発明は、請求項9又は10に対応する発明において、専用デジタル機器に対応するものと、汎用デジタル機器に対応するものとで、形状が異なり相互の交換が不可である半導体装置である。

【0028】本発明は、このような手段を設けたので、請求項4に対応する発明と同様な作用効果が得られる。また、請求項12に対応する発明は、請求項9～11に対応する発明において、専用デジタル機器に対応するものと、汎用デジタル機器に対応するものとで、その

内部処理用のコードが異なり相互の交換が不可である半導体装置である。

【0029】本発明は、このような手段を設けたので、請求項5に対応する発明と同様な作用効果が得られる。さらに、請求項13に対応する発明は、外部より入力したデータ若しくは内部の記録媒体から読み出したデータを暗号化処理する暗号化手段と、この暗号化手段により暗号化されたデータを外部伝送路に出力する送信手段とを有する送信側機器と、外部伝送路を介して暗号化されたデータを受信する受信手段と、この受信手段により受信した暗号化されたデータの復元化処理を行う復号化手段とを有する受信側機器とからなる情報提供システムにおいて、送信手段は受信手段と交信することにより、受信側機器を認識する認識手段を備え、送信手段は認識手段が受信側機器が送信可能な機器であると認識した場合にのみデータの送信を行う情報提供システムである。

【0030】本発明は、このような手段を設けたことにより、まず、送信側機器において外部より入力したデータ若しくは内部の記録媒体から読み出したデータが暗号化手段により暗号化処理される。

【0031】次に通信手段により、受信側機器の受信手段と交信がなされ、その認識手段によりデータ送信すべき受信側機器がどのようなものが認識される。そして相手側の受信側機器が送信可能な機器であると認識された場合にのみ、送信手段により暗号化されたデータが外部伝送路に出力されデータ送信される。

【0032】受信側機器では、受信手段により外部伝送路を介してこの暗号化されたデータが受信され、復号化手段にて暗号化されたデータの復元化処理が行われる。このようにして情報提供システムでは、データ伝送を介在する場合にあっても正しい送信側機器及び受信側機器の組み合わせのときのみデータ伝送が行われ、不用意な不正コピーを防止できることとなる。

【0033】さらにまた、請求項14に対応する発明は、請求項13に対応する発明において、受信側機器は、オーディオヴィジュアル機器等の専用デジタル機器かソフトウェアによりコントロール可能なCPUバスを有するコンピュータ等の汎用デジタル機器の何れか一方であり、認識手段は受信側機器が専用デジタル機器か汎用デジタル機器であるかを認識する情報提供システムである。

【0034】本発明は、このような手段を設けたので、請求項13に対応する発明と同様な作用効果が得られる。他、特に受信側機器がコンピュータ等の汎用デジタル機器である場合に、CPUバス上を流れるデータのコピーによる不正なコピーを防止することが可能となる。

【0035】

【発明の実施の形態】以下、本発明の実施の形態について説明する。

（発明の第1の実施の形態）本発明にかかるデジタル

記録再生システムには、マルチメディア・データをネットワークやケーブルあるいは衛星を介して受信し再生出力する場合やDVD-RAM、D-VCRやCDROM-R等から取り出したデータを再生出力する場合等、種々の形態が考えられる。しかし、何れにしてもどこかの段階で暗号化されたデータをIEEE1394により再生手段本体に伝送し、再生手段本体にて暗号を解いて再生出力することとなる。

【0036】本実施形態では、MPEG2方式で圧縮されたデジタル画像をIEEE1394でつながれたDVD-RAM、D-VCR等の記録取出部分と、記録再生AVの再生部分やパソコン等の再生機器部分と間でやり取りする場合について説明する。

【0037】まず、記録再生AVにより記録再生する場合について説明する。図1は本発明の第1の実施の形態に係るデジタル記録再生システムの一例を示す構成図であり、再生機器部分にDVD-RAM、D-VCR等の専用デジタル記録再生AV機器を用いる場合を示している。

【0038】この専用デジタル記録再生AV機器100においては、送信機器101によりDVD-RAM等から再生対象となるMPEG2画像103が取出されIEEE1394ケーブル105を介して送信される。また、送信機器101から送信されたデータが専用デジタル記録再生AV機器本体である受信機器102によりディスプレイ120に再生出力されるようになっている。

【0039】送信機器101は、DVD-RAM等からデータ圧縮されたMPEG2画像103を取り出す部分(図示せず)と、IEEE1394のインターフェースの送信チップユニット104とから構成される。

【0040】一方、受信機器102は、IEEE1394のインターフェースの受信チップユニット106と、MPEG2画像を復号するための処理部107とから構成される。

【0041】送信チップユニット104は、IEEE1394暗号化部109とIEEE1394I/F部110aを具備する。ここで、各部109、110aは1チップ(1LSI、複合チップを含む)としての送信チップユニット104内に設けられていてもよいし、各部109、110aはそれぞれが1チップであり、送信チップユニット104はこれらのチップセットからなっているともよい。

【0042】一方、受信チップユニット106は、IEEE1394I/F部110bとIEEE1394復号化部111とを具備する。ここで、各部110b、111も送信チップユニット104の場合と同様に、各部110b、111はそれぞれが1チップで受信チップユニット106がこれらのチップセットであっても、各部110b、111が1チップの受信チップユニット106

内に設けられていてもよい。

【0043】また、IEEE1394I/F部110aとIEEE1394I/F部110bとは、IEEE1394インターフェース規格にしたがってIEEE1394ケーブル105を介して両者間でデータ伝送を行うものである。

【0044】ここで、IEEE1394I/F部110bは、自己が設けられるのが専用デジタル記録再生AV機器100であることを認識できる構成となっている。かかる認識はIEEE1394I/F部110bの認識部130によりなされるが、認識部130は、IEEE1394I/F部110bがAV機器用のLSIという情報を保持することで認識するようになっていてもよいし、また、IEEE1394I/F部110bがIEEE1394復号化部111と組み合わせられているということから認識するようになっていてもよい。前述の認識方法は、IEEE1394I/F部110bとIEEE1394復号化部111とが別々のチップとなっているときに特に有効であり、後述の方法はこれらが一体のチップとなっているときに特に有効である。また、その他の認識方法を用いてもよい。

【0045】次に、IEEE1394暗号化部109とIEEE1394復号化部111とによる再生データ103の暗号化及び復号化について説明する。まず、送信機器101内において、MPEG2画像データ103は暗号鍵Sk(108)を用いてIEEE1394暗号化部109により暗号化される。暗号化方式はDESやIDEA等のブロック暗号でも構わないし、ストリーム暗号、公開鍵暗号でも構わない。本実施形態では、暗号化する鍵と復合化する鍵とが同じである共通鍵暗号方式を用いるものとする。なお、公開鍵方式の場合は、受信機器102から公開鍵を送ってもらい、受信機器102の公開鍵で暗号化すれば良い。この場合、受信機器102は自分が保持している秘密鍵により暗号を解くことになる。

【0046】暗号化されたデータは、IEEE1394I/F部110aにおいてIEEE1394で規定されたフォーマットにされる。IEEE1394ケーブル105を介して受信機器102へ送られる。受信機器102ではIEEE1394I/F部110bにおいてデータを受け取り暗号鍵Sk(108)を用いてIEEE1394復号化部111において復号される。

【0047】さて、ここでIEEE1394I/F部110aからIEEE1394I/F部110bへの正常なデータ伝送が実施できるのは、これらが専用デジタル記録再生AV機器用のI/Fセットとして正規なものが装着されているからである。すなわちIEEE1394I/F部110aとIEEE1394I/F部110bとは通信時にお互いの認証を取り合うが、そのときに認識部130の機能によりIEEE1394I/F部1

10bがどのようなものであるかが認識され、当該I/F部110bが専用デジタル記録再生AV機器用のI/F部でなければ通信が行われなくなっている。

【0048】このようにして不正なIEEE1394インターフェースチップが用いられた場合には、送信機器101～受信機器102間の通信ができないようになっているが、受信機器102において受信復号化できた場合にはさらに以下のように処理される。まず、復号されたMPEG2画像データはMPEG2画像を復号するための処理部107において、MPEG2圧縮されたデータがデータ復号部112で解凍される。そして、解答データがD/A変換部113でデジタル信号からアナログ信号に変換されて、例えばディスプレイ装置120へ送られ再生される。

【0049】さて、ここで暗号鍵SkをIEEE1394ケーブル105を介してどのように共有するかについて説明する。この方法については、例えばDVD-ROMにおけるBUSKeyの共有方式を用いればよい。

【0050】このBUSKeyの共有方式については、『ニュースレポートDVD-ROM 装置用の標準インターフェースが固まる暗号鍵の安全な交換手順を規定』、日経エレクトロニクス1996.11.18 (No. 676), pp.13～pp.14 に詳述されている。

【0051】この方法では、まず、受信機器102において乱数発生器などでチャレンジ鍵1(10バイト長)を生成し、送信機器101へ送る。送信機器101では送られたチャレンジ鍵1でKey1(5バイト長)を生成し、受信機器102では同様にチャレンジ鍵1で上記と同じKey1を生成する。Key1の生成は、一方方向関数などを用いて生成される。次に、送信機器101はやはり乱数発生器を用いてチャレンジ鍵2(10バイト長)を生成し、受信機器102へ送る。受信機器102では送られたチャレンジ鍵2を用いてKey2(5バイト長)を生成する。同様に送信機器101では生成したチャレンジ鍵2を用いてKey2を生成する。こうして送信機器101、受信機器102でKey1、Key2が共有できる。そこで、このKey1及びKey2を用いてBUSKeyを生成する。以上のような手順を用いれば、IEEE1394ケーブル105を介して、ケーブル内を暗号化するための鍵をやり取りする必要もなくなり、安全な鍵共有を図ることが可能となる。さらに、このBUSKeyは毎回変わるKey1及びKey2を用いて作成し、有効なのは1回限りである。このようにして安全性を高めている。

【0052】このようにして、専用デジタル記録再生AV機器100の場合には、パーソナルコンピュータと異なりCPUバスを持たないため、暗号を復号する部分と圧縮を復号する部分と受信チップユニット106と処理部107とにわけて構成し、暗号が復号されたデータを圧縮画像の復号部112へ送っても構わない。しか

し、図1の構成をパーソナルコンピュータへ適用すれば、暗号が復号されたデータはCPUバスを経由して圧縮画像の復号部へ送られるため、IEEE1394ケーブル105上を暗号化する意味がなくなってしまう。

【0053】そこで、再生機器部分にパーソナルコンピュータを用いる場合について説明する。図2は本発明の第1の実施の形態に係るデジタル記録再生システムの他の例を示す構成図であり、再生機器部分にパーソナルコンピュータを用いる場合を示している。

【0054】このデジタル記録再生システムにおいては、送信機器201によりDVD-RAM等から再生対象となるMPEG2画像203が取出されIEEE1394ケーブル205を介して送信される。また、送信機器201から送信されたデータがパーソナルコンピュータである受信機器202によりディスプレイ220に再生出力されるようになっている。

【0055】送信機器201は、DVD-RAM等からデータ圧縮されたMPEG2画像203を取り出す部分(図示せず)と、IEEE1394暗号化部209とIEEE1394I/F部210aとからなるIEEE1394のインターフェースの送信チップユニット204とによって構成されている。

【0056】ここで、IEEE1394暗号化部209、IEEE1394I/F部210a、送信チップユニット204は、受信機器202に対応するものとなっている他、図1で説明したIEEE1394暗号化部109、IEEE1394I/F部110a、送信チップユニット104と同様なものとなっている。

【0057】一方、パソコンである受信機器202は、CPUバス240に、CPU241、RAM242、ROM243、IEEE1394のインターフェースの受信チップユニット106及びMPEG2画像を復号するための処理部207が接続されてになっている。

【0058】ここで、CPU241は受信機器202を制御するものであり、RAM242及びROM243はCPU241等の動作において使用されるものである。受信チップユニット206は、IEEE1394I/F部110bからなっており、本実施形態では1チップ(1LSI、複合チップを含む)から構成されている。

【0059】IEEE1394I/F部210bには、認識部230が設けられており、認識部130は、IEEE1394I/F部210bがAV機器用のLSIという情報を保持することで認識するようになっていてもよいし、また、IEEE1394I/F部210bが受信チップユニット206においてIEEE1394復号化部211と組み合わせられていないということから認識するようになっていてもよい。さらにその他の方法でもよい。

【0060】処理部207は、IEEE1394復号化部211と、データ復号部212と、D/A変換部21

3とからなっており、データ復号部212及びD/A変換部213は、図1に示すデータ復号部112及びD/A変換部113と同様に構成されている。

【0061】IEEE1394復号化部211は、暗号を解読し復号化する機能としては図1のIEEE1394復号化部111と同様であるが、その位置が受信チップユニット206でなく処理部207に配置されている。

【0062】送信機器201から受信機器202へのデータ送信における暗号化については、DESやIDEA等のブロック暗号や、ストリーム暗号、公開鍵暗号でも構わない。本実施形態では、専用デジタル記録再生AV機器100の場合と同様、暗号化する鍵と復号化する鍵とが同じである共通鍵暗号方式を用いるものとし、暗号鍵の共有は上記したDVD-ROMにおける鍵共有方式と同様な方式を用いるものとする。

【0063】このように構成されるパソコンを含むデジタル記録再生システムにおいては、まず、DVD-RAM等から取り出されたMPEG2画像データ203がIEEE1394暗号化部209にて暗号化され、専用デジタル記録再生AV機器100の場合と同様にIEEE1394I/F部210aから受信機器202のIEEE1394I/F部210bに送信される。

【0064】ここで暗号化されたデータは、CPUバス240を経由して処理部207へ送られる。したがって、CPUバス240上を流れるデータをコピーしても、データには暗号がかかっており、また、暗号化に用いた鍵(BUSKey)も上述の通り一時的なものである。したがって、CPUバス240上を流れるデータのコピーでは、当該データを再生できず、後に同データを処理部207へ送ったとしてもBUSKeyが一時的なものであるため再生することは不可能である。

【0065】一方、正規にCPUバス240を経由して送られた暗号化されたデータは、送信機器201と共有された暗号鍵Sk(208)を用いて復号化部211において復号される。復号されたMPEG2画像データはデータ復号部212で解凍され、D/A変換部213でデジタル信号からアナログ信号に変換されて、ディスプレイ装置220などへ送られる。

【0066】ところで上記場合に、IEEE1394I/F部210aからIEEE1394I/F部210bへの正常なデータ伝送が実施できるのは、これらに正規なものが装着されているからである。具体的にはパソコンやワークステーション等のソフトウェアでコントロール可能なCPUバスをもつ機器を有するデジタル記録再生システム用のI/Fセットとして正規なものということである。すなわち専用デジタル記録再生AV機器100の場合で説明したように、IEEE1394I/F部210aとIEEE1394I/F部210bとは通信時にお互いの認証を取り合うが、そのときに認識部

230の機能によりIEEE1394I/F部210bがどのようなものであるかが認識される。そして、当該I/F部210bがパソコン等を用いたデジタル記録再生システム用のI/F部でなければ通信が行われないようになっている。

【0067】このように、IEEE1394インターフェースように、コンピュータとAV機器等との統一規格であるインターフェースを用いた場合には、デジタルデータの再生機器部分としては、パソコン等で代表されるソフトウェアでコントロール可能なCPUバスをもつ機器が用いられる場合と、このようなCPUバスをもたない機器が用いられる場合に大別される。図1に示すシステムは前者の再生機器部分が用いられる場合であり、図2に示すシステムは後者の再生機器部分が用いられる場合である。これらの違いは各認識部130、230により区別され、それぞれ対応するI/F部110b、210bが用いられるときのみ正常に動作する。このような区別を確実に行うことによりコンピュータとAV機器等のいずれも接続できるIEEE1394インターフェースにおいて、再生機器部分にコンピュータとAV機器のいずれを用いての確実に両者を区別し、かつそれぞれに対応するやり方で不正コピーを防止できることとなる。

【0068】上述したように、本発明の実施の形態に係るデジタル記録再生システム及び不正コピーを防止する方法は、コンピュータ等とAV機器等のデジタル機器何れかに対応したIEEE1394I/F部110b、210bと、IEEE1394I/F部110a、110bに設けられかつI/F部手段110b、210bが何れのデジタル機器に対応するかを認識可能とする認識部130、230とを具備し、I/F部がその対応するデジタル機器に設けられているときのみ、送信機器101、201と受信機器102、202間で正常なデータ伝送を行うようにしたので、AV機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっては、CPUバス上を流れるデータのコピーによる不正なコピーを防止することができる。

【0069】このように専用の記録再生AV機器と汎用計算機とで受信ユニットを互換性をなくして汎用計算機のCPUバス240上を流れるデータをコピーすることによる不正なコピーを防ぐことができる。

【0070】また、本実施形態の半導体装置は、IEEE1394I/F部110b、210bに認識部130、230が設けられたチップを用いたので、当該半導体装置を使用することで上記効果を得ることができる。

【0071】なお、本実施形態では、D-VC R等の記録機器と、記録再生AV本体やパソコン等の再生機器と間でデータ伝送する場合について説明したが、本発明はこのような場合に限られるものではなく、例えばネット

ワークや衛星通信を介してデータが伝送されてくる場合にも適用できる。例えば衛星からMPEG2圧縮され暗号化されたデータを受信する場合には送信機器101、201に対応するものとしてセットボックス(STB)が設けられることとなるが、セットボックス～受信機器102、202間のIEEE1394によるデータ伝送は、本実施形態の場合と同様に考えることができる。

【0072】また、本発明は、例えばネットワークの接続先が送信機器101、201に対応し、再生画像等使用者側には受信機器102、202に対応する記録再生AV本体やパソコン等の再生機器のみがあるような場合にも適用できる。

(発明の第2の実施の形態) 上記実施形態で説明したように、専用デジタル記録再生AV機器本体とパーソナルコンピュータとで構成を変えたとしても、パソコンを用いる場合に不正コピー者によって、送信チップユニット204と受信チップユニット206のチップセットを送信チップユニット104と受信チップユニット106のチップセットに交換されてしまう場合も考えられる。

【0073】本実施形態は、このような場合に対応するものである。図3は本発明の第2の実施の形態に係るデジタル記録再生システムに使用されるチップ形状の例を示す図である。

【0074】なお、同図に示すチップ形状を除き本実施形態のデジタル記録再生システムは、第1の実施形態の場合と同様に構成されている。図3(a)は、専用デジタル記録再生AV機器用の送信チップユニット104、I/F部110a又は受信チップユニット106、I/F部110bの構成例を示している。一方、図3

(b)は、パーソナルコンピュータを使用するシステム用の送信チップユニット204、I/F部210a又は受信チップユニット206、I/F部210bの構成例を示している。

【0075】このように、専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップの形状として、例えば足の数やボディ部の大きさや形などの形状を変えることで、チップの交換を防止できる。

【0076】上述したように、本発明の実施の形態に係る不正コピーを防止する方法、半導体装置及びデジタル記録再生システムは、専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップの形状として、例えば足の数やボディ部の大きさや形などの形状を変えるようにしたので、半導体装置であるチップの交換を防止でき、第1の実施形態で奏する効果をより一層確実なものとする事ができる。

(発明の第3の実施の形態) 第2の実施形態では、チップ形状を変更することでチップの交換を防止したが、本実施形態は受信機器において、VTR等の専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップの内部処理のコードを変えることにより、

受信ユニット(チップ)の交換を実質的に不可能とするものである。

【0077】具体的には、例えばアスキーコード等のチップ内の制御コマンドの割り当てを、AV機器等用とパソコン等用とで異なったものとする。このように、チップの計上による非互換性だけでなく、内部処理コマンドの違いにより非互換性を担保することができる。

【0078】したがって、制御コマンドの割り当てが異なっているために、もし交換して使用したとすると、外部からの入力に対してチップ内の処理が異なり、正常な動作をしなくなる。そのため、たとえチップを交換できたとしても利用することは不可能である。

【0079】上述したように、本発明の実施の形態に係る不正コピーを防止する方法、半導体装置及びデジタル記録再生システムは、専用デジタル記録再生AV機器とパーソナルコンピュータとで使用されるチップの内部処理のコードを変えるようにしたので、半導体装置であるチップの交換を確実に防止でき、第1の実施形態で奏する効果をより一層確実なものとする事ができる。

【0080】また、本実施形態において、例えばチップにCPUが入っているような場合は、言語をZ80とC言語というように異なる言語を用いることにより、上記と同様の効果を持たせることもできる。

(発明の第4の実施の形態) 第2の実施形態では、チップ形状を変更し、第3の実施形態ではチップ内コードを変更することでチップの交換を防止したが、本実施形態は受信機器において、VTR等の専用デジタル記録再生AV機器とパーソナルコンピュータとで用いられるチップのピンにAV機器等かパソコン等かを識別するピンを設けることで受信ユニット(チップ)の交換を実質的に不可能とするものである。

【0081】具体的には、本実施例のチップは、LSIピンの一つが機器認識用のピンとなっており、このピンから入力される信号により自LSIがAV機器等かパソコン等かの正しい機器に接続されたか否かを自己判定し、正しい機器に接続されていないときには動作しないように構成されている。

【0082】例えば受信機器がパーソナルコンピュータである場合には、上記機器認識用のピンの接続先をダミーとし、ピンに対しては信号入力無しとする。一方、受信機器が専用デジタル記録再生AV機器本体である場合には、一定の信号を入力するようにする。

【0083】したがって、上記一定の信号が入力されるか否かで、チップは自己の対応すべき機器に接続されたかを判定できる。なお、機器認識用のピンへの入力は、AV機器等かパソコン等かで上記場合と逆にしてもよいし、また例えばHレベル、Lレベル信号で区別するようにする等、種々の形態が考えられる。なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【0084】

【発明の効果】以上詳記したように本発明によれば、AV機器等と計算機等との何れもが使用され得る状況にあり、これらの機器に対して暗号化されたデータが送信される場合にあっても、CPUバス上を流れるデータのコピーによる不正なコピーを防止することが可能な不正コピーを防止する方法、及びその半導体装置並びにデジタル記録再生システムを提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係るデジタル記録再生システムの一例を示す構成図。

【図2】本発明の第1の実施の形態に係るデジタル記録再生システムの他の例を示す構成図。

【図3】本発明の第2の実施の形態に係るデジタル記録再生システムに使用されるチップ形状の例を示す図。

【符号の説明】

101…送信機器

102…受信機器（専用デジタル記録再生AV機器本体）

103…MPEG2画像データ

104…送信チップユニット

105…IEEE1394ケーブル

106…受信チップユニット

107…処理部

108…暗号鍵Sk

109…IEEE1394暗号化部

110a…IEEE1394I/F部

110b…IEEE1394I/F部

111…IEEE1394復号化部

112…データ復号部

113…D/A変換部

120…ディスプレイ

130…認識部

201…送信機器

202…受信機器（専用デジタル記録再生AV機器本体）

203…MPEG2画像データ

204…送信チップユニット

205…IEEE1394ケーブル

206…受信チップユニット

207…処理部

208…暗号鍵Sk

209…IEEE1394暗号化部

210a…IEEE1394I/F部

210b…IEEE1394I/F部

211…IEEE1394復号化部

212…データ復号部

213…D/A変換部

220…ディスプレイ

230…認識部

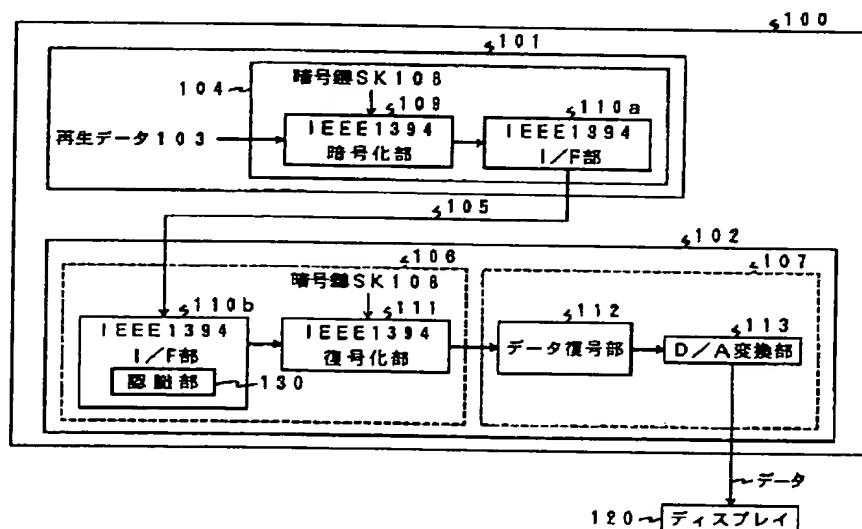
240…CPUバス

241…CPU

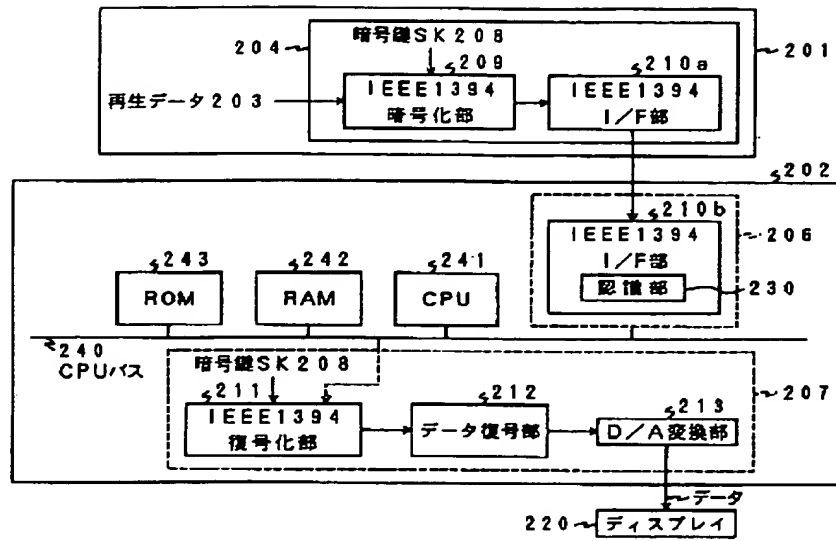
242…RAM

243…ROM

【図1】



【図2】



【図3】

